TEXAS DEPARTMENT OF INFORMATION RESOURCES

Acceptable Use of the Internet, E-Mail, Instant Messages and Peer-to-Peer File Sharing

JULY 24, 2006

Contents

Executive Summary

This guideline is intended to assist state agencies and institutions of higher education compliance with the provisions of the Texas Administrative Code (TAC), Chapter 202 Information Security Standards and Executive Order (RP58) Relating to peer-to-peer file-sharing software. State agencies and institutions of higher education need to assess the associated risks and publish policies to ensure the appropriate use of state systems and networks that provide access to the Internet and technologies used for electronic mail, instant messaging (IM), and peer-to-peer (P2P) file-sharing.

Legislative and judicial branch agencies are not required to follow the provisions of this policy. References to state agencies herein are not intended to cover legislative and judicial branch agencies unless those agencies choose to follow the policy.

Many state employees and users of state-owned information resources rely on access to the Internet to accomplish their jobs, from performing research to communicating directly with the public. The Internet can encourage collaborative projects and resource sharing; aid technological transfer to state businesses; foster innovation and competition within the state; and build a broader infrastructure to support professional, work-related activities. Anyone can abuse the privilege of Internet access, either directly by promoting inappropriate activities and by misusing access time or indirectly by inadvertently allowing unauthorized users to access the network. Internet usage for both personal and professional purposes inherently places state information resources at risk. To protect and operate state information resources properly, all stakeholders must have policies that consider the following:

- **Security**: Protect all data stored or transmitted on state resources
- **Liability**: Avoid downloading illegal, copyrighted and/or unauthorized content.
- **Compliance**: Manage bandwidth usage, personal time and costs, and records retention

State agencies and institutions of higher education must ensure that government computers and the important information they store and transmit remain secure, private, and protected. Each state entity retains the flexibility to develop the most appropriate means of accomplishing this goal through a combination of sound management policies and effective technological means.

Recommendations

All state agencies and institutions of higher education that have not published a policy on Peer-to-Peer file-sharing should initiate actions by August 1, 2006, to publish a policy. The policy must include clearly defined provisions for permitted use, restrictions, and enforcement.

All state agencies and institutions of higher education should consider implementing one or more of the technological measures to control unauthorized P2P and other Internet activity based on the associated risks.

All state agencies and institutions of higher education that have requirements for using collaboration and rapid file sharing technologies should identify and authorize those legitimate tools for their networks. If restricted personal information (an individual's Social Security Number or data protected under state or federal law) is being exchanged, the network/data should be encrypted (see 1 TAC Chapter 202, Information Security Standards).

Managing Risk through Policy and Technology

All state agencies and institutions of higher education should develop practical and enforceable policies regarding acceptable use of the Internet including e-mail, IM, and P2P technologies. Acceptable use policies should take into account agencies' requirements for security, liability and compliance. Each of these areas is explored in more detail below. The example policy statements included in the appendixes contain some statements that may apply to some agencies/institutions, but not others. The specific wording in the example policy statements is, in most instances, purposefully general in nature, allowing management to assume responsibility for defining acceptable practices and exercise full judgement according to their own specific risk assessments.

State entities may choose to have users acknowledge their acceptable use policies in writing, e.g., as part of their initial check in or account creation process. Additional online options for user access policy acknowledgement include banners as part of the user log-on, customized portal applications, government compliance applications, policy awareness and eLearning tools, policy management applications, and Windows domain authentication.

Useful features for these user awareness applications include compliance tracking (tracking access, personal statements and testing), easy access and Web interface searching, an alerting mechanism to warn employees about new threats, templates to facilitate policy creation and updates, and management links to external standards.

Whether acknowledgement is written or electronic, user access policies should consider the following factors:

- Prohibiting personal use of the Internet and e-mail is difficult to enforce. To be effective, any prohibition of unauthorized or illegal use of state information resources must include provisions for monitoring and enforcement.
- State policies should forewarn employees and network users that all Internet activity via state networks or computers is subject to monitoring. Whenever a user accesses the Internet via a state information resource, all activity may be logged and can be used to detect or confirm a user who conducts illegal or unauthorized activity.

Internet monitoring is both a management and a technical issue. The use of state information technology resources is a privilege. If an authorized user fails to comply with this policy or relevant laws and contractual obligations, that user's privilege to access and use state information technology resources may be revoked. Users typically access the Internet through one more of the following channels:

- **Web browsers** are software applications that can locate and display Web pages (Firefox and Internet Explorer are the most common); most can display graphics, text and multimedia, including sound and video.
- **E-mail** is short for electronic mail, the transmission of messages over communications networks that usually have gateways to other computer systems via an Internet Service Provider (ISP).
- **Instant messaging** provides real-time textual communications between individuals using proprietary Internet protocols.
- **Peer-to-peer** file-sharing programs are Internet applications that allow computer users to share electronic files with other users connected to a common file sharing network. P2P represents over 60% of all Internet traffic by data volume, and that figure is growing (see CacheLogic 2004 P2P Traffic Study).

Security

Cyber-terrorists, spies, hackers, and thieves are continually probing Texas systems to steal and profit from our information resources or simply render them useless. Texas state agencies are attacked by more than 88,000 virus attempts per day. That's at least one per second, and the rate is increasing. To cope with the continuous reality of these threats, state agencies must constantly assess vulnerabilities and manage risk to keep networks open and operational, but secure. State agencies and institutions of higher education must ensure that government computers and the important information they store and transmit remain secure, private, and protected. State agencies and institutions of higher education have the flexibility to develop the most appropriate means of accomplishing this goal through a combination of technological means (e.g., Network Address Translation (NAT), "stateful" application firewalls, port and protocol blocking, filtering or shaping, and intrusion prevention systems) and non-technological means (such as policies, monitoring, enforcement, and employee training).

Liability

State agencies and institutions of higher education must consider ethical and legal issues in connection with what is and what is not permissible for state employees to access, distribute electronically, or download to state systems. In adopting policies about the use of state government equipment and networks, state agencies and institutions of higher education should ensure that any permissible personal use:

- Does not unnecessarily place the data stored or transmitted on state resources at risk.
- Does not compromise the security of state infrastructure (i.e., PCs servers or networks)
- Is not used for downloading illegal and/or unauthorized copyrighted content
- Does not result in direct costs paid by the state
- Does not impede agency/institution functions
- Ensures that state resources are not used for private commercial purposes

Before providing access to new employees, state agencies and institutions of higher education must ensure that the employees understand and follow security policies to protect government computers and the important information they store and transmit. According to the Texas Ethics Commission's Ethics Advisory Opinion No. 372:

> Penal Code section 39.02 does not require state agencies to adopt policies absolutely prohibiting any personal use of telephones or computer services as long as the state is reimbursed for any direct costs incurred. In adopting policies about the use of agency equipment, agencies should make sure that any permissible personal use does not result in direct costs paid by the state and does not impede agency functions. Agency policies should also ensure that state resources are not used for private commercial purposes and that only incidental amounts of employee time—time periods comparable to reasonable coffee breaks during the day—are used to attend to personal matters.

The Texas Penal Code also addresses unauthorized computer activities in the following Chapters:

- 16. Criminal Instruments, Interception of Wire or Oral Communication, and Installation of Tracking Device
- 33. Computer Crimes
- 33a. Telecommunications Crimes

Compliance

Compliance with state administrative rules and guidelines requires due diligence in protecting personal information of state citizens, businesses and employees, (e.g., HIPAA and social services directives). As outlined in this policy, personal use of state assets must be limited and reasonable, keeping in mind the intended usage of state assets is to conduct the business of the state in a cost effective manner on behalf of the state's taxpayers.

Any state agency or institution of higher education that uses the Internet, electronic mail and/or file-sharing technologies for official business must also address the management of the associated electronic records of those official transactions. Electronic files are official records subject to state and federal laws for retention and destruction.

Technology Specific Issues

Internet/Web Browsing

Internet Explorer is the most popular browser used for Web browsing (or *surfing*) and is installed by default on each Windows system. Browsers often contain multiple vulnerabilities that can lead to execution of malicious scripts. The most critical vulnerabilities allow remote, unauthorized code execution when an authorized user visits a malicious Web page or reads an HTTP formatted e-mail. Software to exploit these potential vulnerabilities is publicly available, and in some cases, browser vulnerabilities are publicly disclosed and available to cyber criminals before a patch is available ("0-day" vulnerabilities).

These flaws represent opportunities for cyber criminals or terrorists to install spyware, adware and other malware on state systems. Web page spoofing often supports phishing attacks that tempt unsuspecting users to access a malicious or spoofed Web page. Malware is often disguised as a free program that a browser can install on a state government system. The installation of such malware may result in a compromise of the security of those systems or other

computers on the same network and/or propagate to other networks without the knowledge of the user.

Network users can also access streaming media applications such as graphic images and sound files (e.g., Internet radio and other rich media content). As binary stream attachments, these applications have low security risks. However, streaming media consumes large volumes of network resources and can affect user productivity if employees view and listen to personal streaming content during working hours.

E-Mail

E-mail is included within the Transport Control Protocol/Internet Protocol (TCP/IP) suite (e.g., Simple Mail Transfer Protocol (SMTP) for sending e-mail and Post Office Protocol 3 (POP3) for receiving it); both Netscape and Microsoft include an e-mail utility with their Web browsers. Popular e-mail programs include Microsoft's Outlook client, IBM's Lotus Notes, and open source Thunderbird. E-mail vulnerabilities include spam that can overwhelm a network server, inappropriate content that violates social policies, or e-mail attachments or links that execute malicious code.

Instant Messaging

IM services provide real-time textual communications between individuals, however, unlike e-mail, the agency/institution's network default mode has no artifact to document and retain the content of the communications exchange. Without configuring the client to capture and log the traffic, there is no archive record. Much like e-mail, IM can be used to spread computer viruses and for phishing attacks. As e-mail becomes more secure, IM is increasingly a target of hackers and thieves. Unless the agency or institution has an enterprise-wide instant messaging system that provides for managing and archiving IM messages as records, it should have a formal policy prohibiting the use of IM for any official communication that is normally filed for recordkeeping. For additional information see the Texas State Library and Archives Commission Model Policy for Records Management Requirements for Electronic Mail.

Enterprise use of public IM services is approaching 70% of the workforce and is growing both in utilization and importance. IM users report benefiting from faster decisions, higher productivity, and lower telecommunications costs. Concurrently, IM threats are rapidly increasing with reported year over year IM threat increases of 3,266% in the fourth quarter of 2005. IM viruses are transmitted as executable file attachments or as Hyperlinks in IM text directing victims to malicious Web servers. In most cases, these threats require victims to manually execute the virus through social engineering abetted by an unjustified trust in IM buddy lists; or they attack known vulnerabilities for which there is a patch available.

Peer-to-Peer File Sharing

P2P file sharing programs can be used to share any type of electronic files. To accommodate these legitimate file downloads, the State of Texas does not ban P2P programs from its networks. In addition to being the primary channel for malware distribution, one of the primary misuses of P2P technology has been copying of commercial music, movies, and video games for personal enjoyment. These activities on state government systems generally violate the U.S. Copyright

Law and acceptable use policy. Like IM, the effective use and management of P2P for file sharing requires a clear policy, training of employees on the policy, monitoring, and enforcement.

State government computer systems or networks (as well as those operated by contractors on the government's behalf) must not be used to download illegal and/or unauthorized copyrighted content. Any of the following activities constitute violations of acceptable use policy, if done without permission of the copyright owner:

- Copying and sharing images, music, movies, or other copyrighted material using P2P technology
- Making unlicensed copies of a CD or DVD for others
- Posting or plagiarizing copyrighted material
- Downloading any copyright-protected files which you have not already legally procured (e.g., licensed copies of software, MP3s, movies)

Copyright law applies to a wide variety of works and covers much more than what is listed above (see The University of Texas "Crash Course" in Copyright Law).

P2P file-sharing programs increase the connectivity between computers connected to a common P2P network. This heightened connectivity can expose computers to risks beyond those raised by other Internet activities. P2P programs also have a high incidence of being misconfigured to share more folders than the user originally intended. Because P2P file-sharing programs allow all types of electronic data sharing, every computer file in the shared space becomes accessible to every other user on the P2P network. A P2P user who chooses to share a folder containing a music collection may not be aware that he or she is also sharing every personal document that might be stored in the same location.

Viruses and worms can multiply on these P2P networks and enter into a user's computer through a P2P file sharing program. The vast majority of viruses, adware, and Spyware use P2P networks as a primary distribution network. Moreover, free P2P client software often includes adware and backdoors that can be exploited by malware and hackers.

In May 2006, a major media company agreed to use a P2P network best known for illegal downloads to distribute its video content (i.e., Warner Bros. Entertainment via BitTorrent). More P2P distribution of legitimate media is likely and will encourage system developers (e.g., Microsoft and Apple) to integrate P2P applications into the desktop OS. These trends will likely lead to bandwidth congestion and an increased demand to discern between legal and illegal file sharing.

Policy Enforcement

State agencies and institutions of higher education can select from a variety of measures depending on their assessment of risks based on their specific threats, vulnerabilities, and data/system sensitivities. The least intrusive, most positive and effective enforcement measures require a combination of technological means (e.g., "stateful" inspection application firewalls; and blocking, filtering, or shaping systems) and non-technological means, such as written policies, education and awareness, monitoring, and leadership commitment. After closing as many gaps

as possible with technology, the best precaution is to educate users on security practices (e.g., have your IM gateway system send periodic reminders of IM policies).

Technologies to Protect Privacy and Prevent Fraud, Theft, and Disruption

Network Address Translation and Intrusion Prevention Systems (IPS)

Network Address Translation technology reduces the number of direct Internet connections that are visible to outside users or hackers. NAT maps IP addresses from one realm to another and provides transparent routing to hosts. NAT prevents malicious activity initiated by outside hosts from reaching those local hosts. Traditionally, NAT devices are used to connect an isolated address realm with private unregistered addresses to an external realm with globally unique registered addresses. NAT technology can be implemented in a router or firewall and converts internal network addresses to public IP addresses.

Intrusion Prevention/Detection Systems (IPS/IDS) and Anti-virus and Malware Detection Software help block malicious script code. IPS can also help implement access control decisions based on the application content (e.g., video, music, or other file types), rather than IP address or port access. Some IPS can also prevent potentially malicious activity.

Content Filtering Gateways

The best ways to secure networks against Internet/Web browsing vulnerabilities is to install available upgrades and patches, (e.g., Windows XP Service Pack 2), increase the security configuration in Internet Explorer, limit direct exposure to the Internet via NAT, and maintain robust anti-virus, anti-spam, and user privilege programs. Specific best practices also include:

- If possible, enable “Automatic Update” utilities to identify and selectively implement timely system upgrades and patches.
- Implement “Least Privilege” user tools for Internet browsers (e.g., Microsoft “DropMyRights”) to prevent exploitation of remote code execution vulnerabilities at the Administrator level.
- Configure and update anti-virus scanners to detect and remove “Browser Helper Object” spyware programs.
- Put locks on your PCs. Many people leave their computer sessions running all day long; PCs should time out, or log off, automatically with password protection (e.g., after 30 minutes).

Secure Instant Messaging

If Instant Messaging is authorized in writing for your agency/institution, the following best practice and options can help manage IM sessions:

- Configure IM clients to refuse messages from anyone who is not explicitly listed.
- Regular contacts may be infected with an IM-based virus or worm; do not permit selection of any IM link without positive confirmation that a trusted party has sent that link.
- Do not permit file transfers via IM (e.g., through a proxy-based content filter).

Instant Messaging Technology Enforcement Options

The following technologies will help an organization with authorized IM to better control IM protocols and any enabled features, log and audit IM traffic, report IM traffic usage, and better control security vulnerabilities:

- **Keep IM within the firewall.** Closed systems can route instant messages locally, so they never traverse the public network. These systems also offer audit and reporting, virus scanning, directory integration with other e-mail systems, message encryption and user authentication. An Information Resources Manager (IRM) can audit the transcripts and place them in a database.
- **Install a gateway product** that can either route instant messages on the internal enterprise network for employee-to-employee communications or interface with outside IM clients via the Internet. Some gateway products allow IM conversations to be monitored in real time; more common, however, is after-the-fact monitoring of flagged keywords and notifying a manager.
- **Use a proxy server** (discussed in more detail below) between the IM clients on both sides of the firewall to scan for viruses, filter content for sensitive keywords or number patterns (e.g., Social Security Numbers), periodically attach disclaimers to messages, and send all messages to a database for archiving. These systems also allow the IRM to block file transfers, authenticate users, and control IM users.
- **Encrypt messages.** IM systems store instant messages on servers in clear text, which anyone, including hackers, can read. Encryption is one way to bridge this security gap, although it may require both parties to use the same encryption software.

Secure Peer-to-Peer Systems

P2P file sharing technologies can introduce seriously damaging malicious software into an otherwise secure network. Threats such as worms and viruses can easily be introduced into an agency's network, if that network is not specifically protected. P2P file sharing applications can also allow outside users to gain unauthorized access to data and computers on state networks. Most of these P2P applications are designed to evade network controls such as firewalls and proxies. These applications cannot be blocked using simple mechanisms such as destination port and IP address filtering.

P2P file sharing protocols and software take firewall and proxy evasion to a new level. For instance, FastTrack applications such as Kazaa can connect to other FastTrack hosts using any open TCP or UDP port (the same is true for Gnutella applications such as Limewire). Both FastTrack and Gnutella can also transfer files from peer to peer via the standard HTTP protocol, which is simply normal Web traffic, and can pass data and malware through most proxies. This type of P2P protocol can originate from and be directed to any host on the Internet.

IT managers can address the IM and P2P threats by implementing a combination of custom tailored network perimeter defenses such as firewalls, proxies, and routers. However, because of the frequent changes to IM and P2P protocols as well as the ability of IM and P2P traffic to tunnel though or bypass most firewall and proxy configurations, an effective defense must include additional, protocol-aware, signature-based tools.

Recommended Enforcement Approaches

Measures to Manage Peer-to-Peer File Sharing Applications

Some educational institutions have chosen to prohibit the use of P2P file sharing applications that are primarily used for illicit purposes on their networks. For example, the University of Florida developed a network-based system that is flexible enough to provide a continuum of remediation options including education, selective or complete blocking, and track-by-track restriction. The application may be fully customized to manage adherence to a university's own policies. This type of architecture supports other capabilities and addresses the full range of security management issues including viral and worm attacks, spam relays, spyware, botnets, and other outbound malicious behavior. All of these types of malware can have significant effects on the operation and cost effectiveness of the agency or institution of higher education network. The University of Florida reports that this system (marketed under the name "Red Lambda") has been effective in reducing P2P related security issues.

P2P file sharing can also provide outside access to restricted personal information about the individual, other employees, and/or the public. P2P file sharing and IM are often used in state and federal programs to facilitate collaboration between government staff and the public. To reduce the associated risks with these technologies, agencies/institutions should consider running the IM or file sharing system internally or through another government entity.

Other emerging options include the development of licensed P2P networks (such as Penn State's LionShare) which are dedicated to, and specially configured for, the academic network environment. Sharing and distribution of academic material also is available through Web sites, FTP, and e-mail which can be protected using proven policies, procedures, and technologies. Agencies and institutions of higher education can use these standard Internet tools for information sharing and specify exceptions for appropriate use of P2P applications.

Filtering Unauthorized Transmissions

Rather than prohibiting all P2P file sharing or other applications based on a particular protocol or developing an internal P2P system, network filtering systems can filter out unauthorized transmissions by matching them against a master database. One of these commercial systems (CopySense) has been implemented at over 30 educational institutions. It uses an audio fingerprinting technique, allowing the university network to identify, filter, and/or block copyrighted files. This type of content-based filter technology is highly reliable (approximately 99%) and no more intrusive than technologies most schools already employ to scan for viruses and other malware.

Similarly, a filtering appliance can monitor user e-mail for policy violations as well as spam, viruses, or other malware. Content rules can be tailored to incorporate specific personal use policies. When combined with user education, online monitoring can reduce inappropriate as well as damaging content.

Proxy Appliances

Wherever Internet access is available, specifically configured proxy appliances can help address content and URL filtering issues and protect against viruses infiltrating desktops through Web-based back doors—while improving bandwidth management and Web performance. As suggested in the previous sections, proxy appliances can provide network administrators with tools to control, block, log, and bandwidth-limit P2P and streaming media applications. Proxies provide system administrators an ability to control Web communications and protect against risks from spyware, adware, Web viruses, inappropriate Web surfing, IM, video streaming, and P2P file sharing.

A proxy can provide visibility on Web activity and enable administrators to determine the extent of impact these protocols have on network resources. Proxy-generated reports also can enforce Internet access policies and help fine tune them to make best use of the network resources.

Bandwidth Congestion and Shaping

Another option to reduce bandwidth congestion and control unauthorized network activity is to implement a bandwidth shaping tool (e.g., Packeteer). The institutions that have implemented this approach reduce bandwidth allowance during the peak hours of the day, but provide increased bandwidth at night. While this process may reduce unauthorized personal usage to some extent, (e.g., high bandwidth movie downloads or streaming video traffic), it only reduces unauthorized file-sharing during normal working hours. In addition, given the relative small size of music files, most limitations on bandwidth use may still permit the exchange of copyrighted works and will not reduce security threats.

Cost Effectiveness Considerations

The costs associated with implementing any one of these technological measures depends on an agency's network architecture. However, the cost savings from implementing a technological measure may outweigh the expense incurred in implementing them. These cost avoidance considerations include reductions in bandwidth utilization (e.g., the University of Florida experienced an 80% drop in bandwidth utilization after the introduction of the Red Lambda application) and IT infrastructure (the elimination of viruses and other malware accompanying many P2P file sharing applications creates labor and victim notification cost savings).

Appendix A: Example Internet Policy

This policy applies to all forms of Internet use by state employees and does not supersede or limit any state or federal laws, nor any other [agency/institution] policies regarding confidentiality, information dissemination, or standards of conduct. Generally, the Internet should be used for legitimate state business only; however, brief and occasional personal use (i.e., surfing, browsing) is acceptable if the following conditions are met.

Personal Responsibility

Employee personal Internet use on state systems is a privilege, not a right. As such, use should be limited (e.g., personal use could be allowed on a limited basis during lunch or other breaks and during limited periods before and after the employee's regularly scheduled working hours). The privilege may be revoked at any time and for any reason. Abuse of the privilege may result in appropriate disciplinary action.

All authorized users of state networks or systems must use the Internet facilities in ways that do not disable, impair, or overload performance of any other computer system or network, or circumvent any system intended to protect the privacy or security of another user.

Privacy

All users of state networks and systems should keep in mind that all Internet usage can be recorded and stored along with the source and destination. The Internet path record is the property of the [agency/institution]. Such information is subject to the Texas Public Information Act and the laws applicable to state records retention. Employees have no right to privacy with regard to Internet use. Management has the ability and right to view employees' usage patterns and take action to assure that agency Internet resources are devoted to authorized activities and maintain the highest levels of productivity.

Permitted Use

Supervisors should work with employees to determine the appropriateness of using the Internet for professional activities and career development. Written permission is needed and should be obtained for these activities, or the activities should be included in the employee's job description. All users of state networks and systems using the Internet shall identify him/herself honestly, accurately, and completely (including one's affiliation and function where requested) when providing such information.

Only those users of state networks or officials who are expressly authorized to speak to the media or to the public on behalf of the agency may represent the agency via any electronic communication.

If the [agency/institution] [Information Resources Manager or other official] has specifically authorized use of news groups or chat rooms on the state network in writing, state network users may participate in news groups or chat rooms in the course of business when relevant to their duties, but they should do so as individuals speaking for themselves and must include a

disclaimer in their comments similar to the following:

> This message contains the thoughts and opinions of [employee name] and does not represent official [agency/institution name] policy.

Restrictions

Personal Internet use should not impede the conduct of state business; only incidental amounts of employee time—time periods comparable to reasonable coffee breaks during the day—should be used to attend to personal matters.

Accessing, viewing, downloading, uploading, transmitting, printing, copying, posting, or sharing any racist, sexist, threatening, sexually explicit, obscene or otherwise objectionable material (i.e., visual, textual, or auditory entity) is strictly prohibited.

The Internet should not be used for any personal monetary interests or gain.

All users of state networks and systems should not subscribe to mailing lists or mail services strictly for personal use and should not participate in electronic discussion groups (i.e., list server, Usenet, news groups, chat rooms) for personal purposes.

Personal Internet use should not cause the state to incur a direct cost in addition to the general overhead of an Internet connection; consequently, users are not permitted to print or store personal electronic files or material on a state network.

State employees, contractors, and network users must not send, forward, store, or receive confidential agency or institution of higher education information on unapproved mobile devices, such as two-way pagers, personal digital assistants (PDAs), or cell phones. State agency-approved mobile devices may receive and store confidential information in encrypted form.

Acknowledgement

If you have questions about the above policies and procedures, address them to the [appropriate agency/institution Compliance Officer] before signing the following agreement.

I have read the [agency/institution] Internet policy and agree to abide by it. I understand that a violation of any of the above policies or procedures may result in disciplinary action.

_____
User Name

_____
User Signature

_____
Date

This example is for informational purposes only. Individual electronic policies should be developed with assistance from legal counsel.

Appendix B: Example E-Mail Policy

This policy applies to e-mail used within the [agency/institution] and e-mail used conjointly with the Internet and does not supersede any state or federal laws or any other agency policies regarding confidentiality, information dissemination, or standards of conduct. Generally, e-mail should be used only for legitimate state business; however, brief and occasional e-mail messages of a personal nature may be sent and received if the following conditions are met.

Personal Responsibility

Personal use of e-mail is a privilege, not a right. As such, the privilege may be revoked at any time and for any reason. Abuse of the privilege may result in appropriate disciplinary action.

Privacy

All users of state computers and networks should keep in mind that all e-mail can be monitored, recorded, reviewed, and stored along with the source and destination. Employees have no right to privacy with regard to e-mail. Management has the ability and right to view employees' e-mail. Recorded e-mail messages are the property of the [agency/institution]. Thus, they are subject to the requirements of the Texas Public Information Act and the laws applicable to state records retention.

Permitted Use

E-mail messages are official records and are subject to state and agency/institution rules and policies for retention and deletion.

E-mail that contains an individual's name along with any restricted personal information (e.g., Social Security number) will be encrypted for transmission and storage. Users should contact their IT department for appropriate encryption tools and procedures.

Incidental amounts of employee time—time periods comparable to reasonable coffee breaks during the day—can be used to attend to personal matters via e-mail or other telecommunications, similar to personal telephone calls.

All users of state networks and systems should be aware that when sending an e-mail message or other electronic transmission of a personal nature, there is the danger of the employee's words being interpreted as official agency policy or opinion. Therefore, when an employee sends a personal e-mail, especially if the content of the e-mail could be interpreted as an official agency statement, the employee should use the following disclaimer at the end of the message:

> This e-mail contains the thoughts and opinions of [employee name] and does not represent official [agency/institution name] policy.

Restrictions

Personal e-mail use should not impede the conduct of state business.

Accessing, viewing, downloading, uploading, transmitting, printing, copying, posting, or sharing

any racist, sexist, threatening, sexually explicit, obscene or otherwise objectionable material (i.e., visual, textual, or auditory entity) is strictly prohibited.

Individuals must not send, forward or receive confidential or sensitive agency information through non-agency e-mail accounts (e.g., Yahoo!, AOL, or any other e-mail service belonging to an Internet service provider).

E-mail should not be used for any personal monetary interests or gain.

Network users should not subscribe to mailing lists or mail services strictly for personal use.

Personal e-mail should not cause the state to incur a direct cost in addition to the general overhead of e-mail. Consequently, upon receiving personal e-mail, employees should read and delete it.

Acknowledgement

If you have questions about the above policies and procedures, address them to the [appropriate agency/institution Compliance Officer] before signing the following agreement.

I have read the [agency/institution] e-mail policy and agree to abide by it. I understand that a violation of any of the above policies or procedures may result in disciplinary action.

_____
User Name

_____
User Signature

_____
Date

This example is for informational purposes only. Individual electronic policies should be developed with assistance from legal counsel.

Appendix C: Example Instant Messaging Policy

Employees will not download/install any Instant Messaging (IM) software without specific authorization in writing from the [agency/institution] [Information Resources Manager (IRM) or title of other specific individual authorized to grant IM implementation].

Employees authorized to use IM technologies will not download any illegal and/or unauthorized copyrighted content. The [IRM or title of other specific individual authorized to grant IM implementation] must approve the use of IM technology to download copyrighted material in writing. The state entity must follow appropriate state and federal laws and guidelines when copying, storing, or transferring copyrighted material.

This policy applies to IM used within the agency or institution and IM used conjointly with the Internet and does not supersede any state or federal laws, or any other agency policies regarding confidentiality, information dissemination, or standards of conduct. Generally, IM should be used only for legitimate state business; however, brief and occasional IM of a personal nature may be sent and received if the following conditions are met.

Personal Responsibility

Personal use of IM is a privilege, not a right. As such, the privilege may be revoked at any time and for any reason. Abuse of the privilege may result in appropriate disciplinary action.

Privacy

Authorized state network users should keep in mind that all IM can be recorded and stored along with the source and destination. Users have no right to privacy with regard to IM. Management has the ability and right to view employees' IM. Recorded instant messages are the property of the [agency/institution]. Thus, they are subject to the requirements of the Texas Public Information Act and the laws applicable to state records retention.

Personal Use

Incidental amounts of employee time—time periods comparable to reasonable coffee breaks during the day—can be used to attend to personal matters via IM or other telecommunications, similar to personal telephone calls.

Restrictions

Personal IM should not impede the conduct of state business.

If authorized for usage on state systems, IM may be used for any routine official business communication that is not normally filed for recordkeeping, such as a communication that is temporarily needed only for an employee to complete an action.

Do not use IM to conduct any state business that would require the content to be saved as a state record. IM may not be used to document a statutory obligation or agency decision, and IM should not be used when the resulting record would normally be retained for recordkeeping purposes.

Accessing, viewing, downloading, uploading, transmitting, printing, copying, posting, or sharing any racist, sexist, threatening, sexually explicit, obscene, or otherwise objectionable material (i.e., visual, textual, or auditory entity) is strictly prohibited.

IM should not be used for any personal monetary interests or gain.

Acknowledgement

If you have questions about the above policies and procedures, address them to the [appropriate agency/institution Compliance Officer] before signing the following agreement.

I have read the [agency/institution] IM policy and agree to abide by it. I understand that a violation of any of the above policies or procedures may result in disciplinary action.

_____
User Name

_____
User Signature

_____
Date

This example is for informational purposes only. Individual electronic policies should be developed with assistance from legal counsel.

Appendix D: Example Peer-to-Peer Policy for State Agencies

This policy applies to Peer-to-Peer (P2P) used within the [agency] and P2P used conjointly with the Internet and does not supersede any state or federal laws, or any other agency policies regarding confidentiality, information dissemination, or standards of conduct. Generally, P2P should be used only for legitimate state business; however, brief and occasional P2P of a personal nature may be sent and received if the following conditions are met.

Users of state computers or networks that are authorized to use P2P technologies will not download any illegal and/or unauthorized copyrighted content. The [Information Resources Manager (IRM) or other specific individual authorized to grant P2P network implementation/installation] must approve the use of P2P technology to download copyrighted material in writing. State users must follow appropriate state and federal laws and guidelines when copying, storing, or transferring copyrighted material.

If authorized for usage on state systems, P2P may be used for any routine official business communication that is not normally filed for recordkeeping, such as a communication that is temporarily needed only for an employee to complete an action.

Personal Responsibility

Users of state computers or networks shall not download/install or use any P2P software on state computers, networks, or mobile computing device (PDA) without specific authorization in writing from the [agency] [IRM or title of other specific individual authorized to grant P2P implementation].

Personal use of P2P is a privilege that must be granted specifically in writing by [an authorized official]. As such, the privilege may be revoked at any time and for any reason. Abuse of the privilege may result in appropriate disciplinary action.

Authorized network users may use P2P technologies for official business only if specifically authorized in writing by the [appropriate state agency official].

If any copied or transferred data or information is licensed or copyrighted, the [authorizing official] and authorized network user shall ensure that all notifications and costs are documented and approved.

Privacy

Users of state computers and networks should keep in mind that all P2P may be recorded and stored along with the source and destination. Employees have no right to privacy with regard to P2P. Management has the ability and right to view users' P2P on state systems.

P2P files recorded on state systems are the property of the [agency]. Thus, they are subject to the requirements of the Texas Public Information Act and the laws applicable to state records retention.

Personal Use

If authorized in writing by [the appropriate official], incidental amounts of employee time—time periods comparable to reasonable coffee breaks during the day—may be used to attend to personal matters via P2P, similar to personal telephone calls. Personal P2P use should not cause the state to incur a direct cost in addition to the general overhead of an Internet connection; consequently, users are not permitted to print or store personal electronic files or material on a state network.

Restrictions

Personal P2P use should not impede the conduct of state business; only incidental amounts of employee time—time periods comparable to reasonable coffee breaks during the day—should be used to attend to personal matters.

Accessing, viewing, downloading, uploading, transmitting, printing, copying, posting, or sharing any racist, sexist, threatening, sexually explicit, obscene, or otherwise objectionable material (i.e., visual, textual, or auditory entity) is strictly prohibited.

P2P should not be used for any personal monetary interests or gain.

Acknowledgement

If you have questions about the above policies and procedures, address them to the [appropriate agency Compliance Officer] before signing the following agreement.

I have read the [agency] P2P policy and agree to abide by it. I understand that a violation of any of the above policies or procedures may result in disciplinary action.

_____
User Name

_____
User Signature

_____
Date

This example is for informational purposes only. Individual electronic policies should be developed with assistance from legal counsel.

Appendix E: Example Peer-to-Peer Policy for Institutions of Higher Education

This policy applies to Peer-to-Peer (P2P) used within the institution and P2P used conjointly with the Internet and does not supersede any state or federal laws, or any other [state institution] policies regarding confidentiality, information dissemination, or standards of conduct. Employees or contractors can use P2P for legitimate state or institution business if authorized by the [Information Resources Manager (IRM) or other specific individual authorized to grant P2P network implementation/installation].

The [IRM or other specific individual authorized to grant P2P network implementation/installation] must approve the use of P2P technology to download copyrighted material in writing. [State institution] network users must follow appropriate state and federal laws and guidelines when copying, storing, or transferring copyrighted material (e.g., automated software patch updates/upgrades). Users of [state institution] computers or networks that use P2P (or other file sharing technologies) to download illegal and/or unauthorized copyrighted content are subject to legal and administrative sanctions.

If authorized for usage on state systems, P2P may be used for any routine official business communication that is not normally filed for recordkeeping, such as a communication that is temporarily needed only for an employee to complete an action.

State institutions will cooperate in investigating and resolving any non-compliance or infringement issues and will take such action as reasonably requested by complainant to terminate or correct such non-compliance or infringement. The institution will be responsible to the same extent it would otherwise be responsible under federal copyright law for harms that might result from its failure to comply with the provisions of this policy.

Personal Responsibility

Users of state computers or networks shall not download/install any P2P software onto state computers, networks, or mobile computing device (PDA) without specific authorization in writing from the [state institution] [IRM or title of other specific individual authorized to grant P2P implementation].

Personal use of P2P on state institution-owned computers and networks is a privilege that must be granted specifically in writing by [an authorized official]. As such, the privilege may be revoked at any time and for any reason. Abuse of the privilege may result in appropriate administrative or disciplinary action.

Authorized network users may use P2P technologies for official business only if specifically authorized in writing by [the appropriate state institution official].

If any copied or transferred data or information is licensed or copyrighted, the [authorizing official] and authorized network user will ensure that all notifications and costs are documented and approved.

Privacy

Users of state institution computers and networks should keep in mind that all P2P may be recorded and stored along with the source and destination. Employees have no right to privacy with regard to P2P usage on [state institution] computers and networks. Management has the ability and right to view users' P2P on state institution systems. P2P files recorded onto state institution computers or networks are the property of the institution. Thus, they are subject to the requirements of the Texas Public Information Act and the laws applicable to state records retention.

Personal Use

Additionally, authorized users of the [state institution's] network may send and receive P2P of a personal nature if the following conditions are met.

If authorized in writing by [the appropriate official], incidental amounts of employee time—time periods comparable to reasonable coffee breaks during the day—may be used to attend to personal matters via P2P, similar to personal telephone calls.

Personal P2P use should not cause the state to incur a direct cost in addition to the general overhead of an Internet connection; consequently, employees are not permitted to print or store personal electronic files or material on a [state institution] computer or network.

Authorized users of the [state institution] network (e.g., students) may use permitted P2P technologies to legally download files onto personally owned computers using available bandwidth and connectivity, with the expectation that there will be no cost to the institution.

Restrictions

Personal use of P2P should not impede the conduct of [state institution] business.

Accessing, viewing, downloading, uploading, transmitting, printing, copying, posting, or sharing any racist, sexist, threatening, sexually explicit, obscene, or otherwise objectionable material (i.e., visual, textual, or auditory entity) on [state institution] computers or networks is strictly prohibited.

Employees should not use P2P on state computers or networks for any personal monetary interests or gain.

Acknowledgement

If you have questions about the above policies and procedures, address them to the [appropriate institution Compliance Officer] before signing the following agreement.

I have read the [state institution] P2P policy and agree to abide by it. I understand that a violation of any of the above policies or procedures may result in disciplinary action.

_____

User Name

_____

User Signature

_____

Date

This example is for informational purposes only. Individual electronic policies should be developed with assistance from legal counsel.